EXHIBIT 1

AO 93 (SDNY Rev. 01/17) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Two Email Accounts, Two iCloud Accounts, and Two iPhones Currently Located on Four Hard Drive Partitions Containing the Results of Prior Search Warrants

Case No. 20MAG00740

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Southern District of New York
(identify the person or describe the property to be searched and give its location):

See Attachment A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment A

The search and seizure are related to violation(s) of *(insert statutory citations)*:

18 U.S.C. § 1343 (wire fraud) and § 1349 (attempting and/or conspiring to commit wire fraud)

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before February 4, 2020
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Clerk of the Court.

☒ Upon its return, this warrant and inventory should be filed under seal by the Clerk of the Court. JPO
USMJ Initials

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: Jan. 21, 2020 5:00 pm

Judge's signature

City and state: New York, NY

J. Paul Oetken, United States District Judge
Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the Court.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

Attachment A

I. Devices to be Searched

The devices to be searched ("Subject Device-1," "Subject Device-2," "Subject Device-3," and "Subject Device-4," and collectively, the "Subject Devices") are described as four hard drive partitions containing the following content and information obtained pursuant to the following prior search warrants:

Account/Device	Previously searched pursuant to search warrant(s)	Referred to as
SUBJECT DEVICE-1		
[redacted]	19 Mag. 729 (Jan. 18, 2019) 19 Mag. 7593 (Aug. 14, 2019)	Parnas Yahoo Account
[redacted]	19 Mag. 7595 (Oct. 17, 2019)	Correia Yahoo Account
SUBJECT DEVICE-2		
Parnas iCloud account number [redacted]	19 Mag. 4784 (May 16, 2019) 19 Mag. 9829 (Oct. 21, 2019)	Parnas iCloud Accounts
iCloud account number [redacted]	19 Mag. 9832 (Oct. 21, 2019)	
SUBJECT DEVICE-3		
Black iPhone 11 with the serial number [redacted] seized from Lev Parnas incident to his arrest at Dulles International Airport on Oct. 9, 2019	19 Mag. 9832 (Oct. 21, 2019)	Parnas iPhone 11
SUBJECT DEVICE-4		
iPhone with the serial number [redacted] seized from a package sent by David Correia via DHL	19 Mag. 9830 (Oct. 21, 2019)	Correia iPhone

II. Review of ESI on the Subject Devices

Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, interpreters, and outside vendors or technical experts under government control) are authorized to review the ESI contained on the Subject Devices for evidence, fruits, and instrumentalities of one or more violations of 18 U.S.C. § 1343 (wire fraud) and § 1349 (attempting and/or conspiring to commit wire fraud) (together, the "Subject Offenses"), limited to content created, sent, or received between September 1, 2013 and the date of this warrant, as listed below:

a. Evidence relating to, including communications with, Rudolph Giuliani, [redacted] and any actual or potential investors, members, or partners of Fraud Guarantee;

b. Evidence relating to Fraud Guarantee's plans, finances, assets, and operations, or lack thereof, including any corporate books and records;

c. Evidence relating to Fraud Guarantee's actual or prospective business relationships, including but not limited to business relationships with any insurance carriers;

d. Evidence relating to Fraud Guarantee's members, officers, directors, investors, partners, employees, agents, consultants, affiliates, subsidiaries, and associates.

e. Evidence relating to the nature and extent of Rudolph Giuliani's and [redacted] work on behalf of Parnas, Correia, and/or Fraud Guarantee, or lack thereof, including any evidence of Giuliani's efforts to assist in the removal of Ambassador [redacted] and whether or not such efforts benefited Fraud Guarantee;

f. Evidence relating to any efforts by Parnas, Correia, their family members, or others associated with Fraud Guarantee in receiving, transferring, withdrawing, or otherwise using any monetary funds or instruments;

g. Evidence relating to the use of monetary funds or instruments paid to Fraud Guarantee, Parnas, or Correia to make political contributions;

h. Evidence of meetings between Parnas, Correia, Giuliani, and any actual or potential investors in Fraud Guarantee, including but not limited to travel records, and location and IP records;

i. Evidence of the existence of email accounts, iCloud accounts, or electronic devices used by Parnas, Correia or others associated with Fraud Guarantee to communicate with actual or potential investors, or co-conspirators;

j. Passwords or other information needed to access user's online accounts.

UNITED STATES DISTRICT COURT

for the

Southern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Two Email Accounts, Two iCloud Accounts, and Two iPhones on Four Hard Drive Partitions

Case No. 20 MAG 00740

APPLICATION FOR A SEARCH AND SEIZURE WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attached Affidavit and its Attachment A

located in the Southern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

See Attached Affidavit and its Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section(s)	*Offense Description(s)*
See Attached Affidavit and its Attachment A	

The application is based on these facts:

See Attached Affidavit and its Attachment A

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: ____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[redacted]

Applicant's signature

Sworn to before me and signed in my presence.

Date: 01/21/2020

Judge's signature

City and state: New York, NY

J. Paul Oetken, United States District Judge

Printed name and title

20 MAG 00740

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States Of America for a Search Warrant for the Contents of Two Email Accounts, Two iCloud Accounts, and Two iPhones Currently Located on Four Hard Drive Partitions Containing the Results of Prior Search Warrants, USAO Reference No [redacted]

TO BE FILED UNDER SEAL

Agent Affidavit in Support of Application for a Search Warrant

SOUTHERN DISTRICT OF NEW YORK) ss.:

[redacted], being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). In the course of my experience and training in this position, I have participated in criminal investigations into federal offenses involving public corruption and violations of the federal campaign finance laws. I also have training and experience executing search warrants, including those involving electronic evidence, including emails.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search (i) two email accounts on an electronic device specified below ("Subject Device-1"), (ii) two iCloud accounts on a second electronic device specified below ("Subject Device-2"), (iii) an iPhone 11 on a third electronic device specified below ("Subject Device-3"), and (iv) an iPhone on a fourth electronic device specified below ("Subject Device-4" and, collectively, the "Subject Devices"), for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and

the forensic analysis of electronically stored information ("ESI"). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. Prior Warrants and the Subject Devices

3. Subject Device-1 is a hard drive partition in the possession of the FBI and U.S. Attorney's Office for the Southern District of New York ("USAO") which contains the results of search warrants for the email account [redacted] used by Lev Parnas (the "Parnas Yahoo Account") and the email account [redacted]m used by David Correia (the "Correia Yahoo Account"). More specifically:

a. The Parnas Yahoo Account and Correia Yahoo Account have previously been searched pursuant to the following search warrants:

Search warrant date and docket number	**Target of search**	**Subject offenses**
Jan. 18, 2019 19 Mag. 729	Parnas Yahoo Account and Correia Yahoo Account (among other email accounts)	52 U.S.C. § 30122 (unlawful straw donations), 52 U.S.C. § 30121 (unlawful foreign contributions), 18 U.S.C. § 371 (conspiracy to commit the same), 18 U.S.C. § 2 (aiding and abetting the same), 18 U.S.C. § 1343 (wire fraud), and 18 U.S.C. § 1956 (money laundering)

Aug. 14, 2019 19 Mag. 7593	Parnas Yahoo Account and Correia Yahoo Account (among other email accounts)	52 U.S.C. § 30122 (unlawful straw donations), 52 U.S.C. § 30121 (unlawful foreign contributions), 18 U.S.C. § 371 (conspiracy to commit the same), 18 U.S.C. § 2 (aiding and abetting the same), 18 U.S.C. § 1001 (false statements in a matter within the jurisdiction of the executive branch), 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1346 (honest services fraud), 18 U.S.C. § 1956 (money laundering), 22 U.S.C. §§ 612, 618 (failure to register as an agent of a foreign principal violation), 18 U.S.C. § 951 (acting as an agent of a foreign government), 18 U.S.C. § 201 (bribery); and 18 U.S.C. § 203 (bribery with respect to a member of congress)
Oct. 17, 2019 19 Mag. 7595	Two devices containing the returns from the January 18, 2019 warrant (19 Mag. 729)	18 U.S.C. § 1001 (false statements in a matter within the jurisdiction of the executive branch), 18 U.S.C. § 1346 (honest services fraud), 22 U.S.C. §§ 612, 618 (failure to register as an agent of a foreign principal violation), 18 U.S.C. § 951 (acting as an agent of a foreign government), 18 U.S.C. § 201 (bribery); and 18 U.S.C. § 203 (bribery with respect to a member of congress)

b. The content and information associated with the Parnas Yahoo Account and Correia Yahoo Account have been loaded onto Subject Device-1. As detailed herein, by this application, the Government seeks authorization to expand the scope of its search of these two accounts contained on Subject Device-1.

4. Subject Device-2 is a hard drive partition in the possession of the FBI and USAO which contains the results of search warrants for an iCloud account with identification number [redacted] and an iCloud account with identification number [redacted], both used by Lev Parnas (the "Parnas iCloud Accounts"). More specifically:

a. The Parnas iCloud Accounts have previously been searched pursuant to the following search warrants:

Search warrant date and docket number	**Target of search**	**Subject offenses**
May 16, 2019 19 Mag. 4784	Parnas iCloud Accounts (among other iCloud accounts)	52 U.S.C. § 30122 (unlawful straw donations), 52 U.S.C. § 30121 (unlawful foreign contributions), 18 U.S.C. § 371 (conspiracy to commit the same), 18 U.S.C. § 2 (aiding and abetting the same), 18 U.S.C. § 1001 (false statements in a matter within the jurisdiction of the executive branch), 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1346 (honest services fraud), and 18 U.S.C. § 1956 (money laundering)
Oct. 21, 2019 19 Mag. 9829	Parnas iCloud Accounts (among other iCloud accounts)	52 U.S.C. § 30122 (unlawful straw donations), 52 U.S.C. § 30121 (unlawful contribution by a foreign national), 18 U.S.C. § 371 (conspiracy to commit the same), 18 U.S.C. § 2 (aiding and abetting the same), 18 U.S.C. § 1001 (false statement to the Federal Election Commission ("FEC")), and 18 U.S.C. § 1001 and 2 (willfully causing a false statement to be made to the FEC), 18 U.S.C. § 1519 (fabrication of documents); 22 U.S.C. §§ 612 and 618 (failure to register as a foreign agent); 18 U.S.C. § 951 (acting as an agent of a foreign government); 18 U.S.C § 1956 (international promotional money laundering); and 18 U.S.C. § 1343 (wire fraud)
Oct. 21, 2019 19 Mag. 9832	A device containing selected results of the May 16, 2019 warrant (19 Mag. 4784)	18 U.S.C. § 1519 (fabrication of documents); 22 U.S.C. §§ 612 and 618 (failure to register as a foreign agent); 18 U.S.C. § 951 (acting as an agent of a foreign government); and 18 U.S.C. § 1343 (wire fraud)

b. The content and information associated with the Parnas iCloud Accounts have been loaded onto Subject Device-2. As detailed herein, by this application, the Government seeks authorization to expand the scope of its search of these two accounts contained on Subject Device-2.

5. Subject Device-3 is a hard drive partition in the possession of the FBI and USAO which contains the results of a search warrant for a black iPhone 11 with the serial number [redacted] seized from Lev Parnas incident to his arrest at Dulles International Airport on or about October 9, 2019 (the "Parnas iPhone 11"). More specifically:

a. The Parnas iPhone 11 has previously been searched pursuant to the following search warrant:

Search warrant date and docket number	**Target of search**	**Subject offenses**
Oct. 21, 2019 19 Mag. 9832	Parnas iPhone 11 (among other devices)	52 U.S.C. § 30122 (unlawful straw donations), 52 U.S.C. § 30121 (unlawful contribution by a foreign national), 18 U.S.C. § 371 (conspiracy to commit the same), 18 U.S.C. § 2 (aiding and abetting the same), 18 U.S.C. § 1001 (false statement to the FEC, and 18 U.S.C. § 1001 and 2 (willfully causing a false statement to be made to the FEC), 18 U.S.C. § 1519 (fabrication of documents); 22 U.S.C. §§ 612 and 618 (failure to register as a foreign agent); 18 U.S.C. § 951 (acting as an agent of a foreign government); 18 U.S.C § 1956 (international promotional money laundering); and 18 U.S.C. § 1343 (wire fraud)

b. Based on my review of technical information associated with the Parnas iPhone 11, it appears that the Parnas iPhone 11 is a dual-SIM phone and can switch between two separate mobile networks. In particular, the Parnas iPhone 11 has been used to make and receive telephone calls, and send and receive text messages, from two telephone numbers: [redacted] (the "Parnas Numbers").

c. The content and information associated with the Parnas iPhone 11 has been loaded onto Subject Device-3. As detailed herein, by this application, the Government seeks authorization to expand the scope of its search of this device contained on Subject Device-3.

6. Subject Device-4 is a hard drive partition in the possession of the FBI and USAO which contains the results of a search warrant for an iPhone XR with the serial number [redacted] seized from a package sent by David Correia via DHL (the "Correia iPhone"). More specifically:

a. The Correia iPhone has previously been searched pursuant to the following search warrant:

Search warrant date and docket number	**Target of search**	**Subject offenses**
Oct. 21, 2019 19 Mag. 9830	A DHL package sent by David Correia (containing the Correia iPhone, among other things)	52 U.S.C. § 30122 (unlawful straw donations), 52 U.S.C. § 30121 (unlawful contribution by a foreign national), 18 U.S.C. § 371 (conspiracy to commit the same), 18 U.S.C. § 2 (aiding and abetting the same), 18 U.S.C. § 1001 (false statement to the FEC, and 18 U.S.C. § 1001 and 2 (willfully causing a false statement to be made to the FEC), 18 U.S.C. § 1519 (fabrication of documents); 22 U.S.C. §§ 612 and 618 (failure to register as a foreign agent); 18 U.S.C. § 951 (acting as an agent of a foreign government); 18 U.S.C § 1956 (international promotional money laundering); and 18 U.S.C. § 1343 (wire fraud)

b. Based on my review of technical information associated with the Correia iPhone, it appears that the Correia iPhone has been used to make and receive telephone calls, and send and receive text messages, from the telephone number [redacted] (the "Correia Number").

c. The content and information associated with the Correia iPhone has been loaded onto Subject Device-4. As detailed herein, by this application, the Government seeks authorization to expand the scope of its search of this device contained on Subject Device-4.

C. The Subject Offenses

7. In the course of reviewing the content contained on the Parnas Yahoo Account, Correia Yahoo Account, Parnas iCloud Accounts, Parnas iPhone 11, and Correia iPhone (collectively, the "Subject Accounts and Phones") pursuant to the respective search warrants set forth above, as well as my continuing involvement in this investigation, I have discovered materials which, as set forth in greater detail below, establish probable cause to believe the Subject Accounts and Phones contain evidence of additional offenses. I am therefore requesting authority to search the Subject Devices—which contain the content and information from the Subject Accounts and Phones—for evidence, fruits, and/or instrumentalities of these additional offenses.

8. In particular, I respectfully submit that there is probable cause to believe that the Subject Accounts and Phones also contain evidence, fruits, and/or instrumentalities of the commission of 18 U.S.C. § 1343 (wire fraud) and § 1349 (attempting and/or conspiring to commit wire fraud) (together, the "Subject Offenses") in relation to Lev Parnas's and David Correia's involvement in a wire fraud scheme involving a company known as "Fraud Guarantee."

II. Probable Cause Regarding the Subject Offenses

9. On or about October 9, 2019, a grand jury sitting in the Southern District of New York returned an indictment charging defendants Lev Parnas and Igor Fruman with conspiring to make contributions in connection with federal elections in the names of others, in violation of 18 U.S.C. § 371 and 52 U.S.C. §§ 30122 and 30109; and with making false statements and falsifying records to obstruct the administration of a matter within the jurisdiction of the Federal Election Commission, in violation of 18 U.S.C. §§ 1001 and 1519. Additionally, the same indictment

charges Parnas, Fruman, David Correia, and Andrey Kukushkin with conspiring to violate the ban on foreign donations and contributions in connection with federal and state elections, in violation of 18 U.S.C. § 371 and 52 U.S.C. §§ 30121, 30122, and 30109.

10. In addition to prosecuting Parnas, Fruman, Correia, and Kukushkin for the above-referenced crimes, the FBI and USAO are investigating, among other things, whether Parnas and Correia, and others known and unknown, perpetrated a fraudulent scheme through their efforts to raise funds ostensibly for their business "Fraud Guarantee," in violation of 18 U.S.C. §§ 1343 and 1349 (wire fraud and attempt/conspiracy to commit the same). In sum, the evidence provides probable cause to believe that Parnas and Correia solicited multiple investors to contribute hundreds of thousands of dollars to Fraud Guarantee based on materially false explicit and implicit representations regarding the Fraud Guarantee business, including its finances, leadership, and relationship with Rudolph Giuliani and his firm, [redacted]

11. Attached hereto as Exhibit A, and incorporated by reference herein, is a search warrant for Parnas's and Correia's Fraud Guarantee email accounts (19 Mag. 11651), along with the supporting affidavit which describes in detail the basis for determining that there is probable cause to believe that Parnas and Correia committed the Subject Offenses. *See* Exhibit A (affidavit) ¶¶ 8-24.

III. Probable Cause Regarding the Subject Devices

12. Based on the foregoing (including Exhibit A), the facts set forth below, and my training and experience, there is probable cause to believe that the Subject Devices—which contain the content and information from the Subject Accounts and Phones—will contain evidence and instrumentalities of the Subject Offenses, including communications between Parnas and Correia regarding Fraud Guarantee, communications with actual or potential investors in Fraud Guarantee,

and communications with third-party consultants to Fraud Guarantee, including Rudolph Giuliani and his firm, [redacted]

Subject Device-1
(Containing the Parnas Yahoo Account and Correia Yahoo Account)

13. Based on my review of emails from the Parnas Yahoo Account and Correia Yahoo Account (obtained pursuant to the search warrants identified above), and materials produced by witnesses, I have learned, in substance and in part, that Parnas used the Parnas Yahoo Account and that Correia used the Correia Yahoo Account in connection with their scheme involving Fraud Guarantee. For example:

a. On or about June 8, 2015, Correia (using the Correia Yahoo Account) emailed the individual who served as the Chief Executive Officer of Fraud Guarantee (the "CEO") regarding efforts to obtain a deal with an insurance carrier for Fraud Guarantee.

b. On or about January 4, 2016, Correia (copying himself at the Correia Yahoo Account) emailed Parnas (at the Parnas Yahoo Account) regarding, among other things, certain items to address for Fraud Guarantee, including referencing a potential impending investment from a certain individual ("Victim-1").

c. In or about March 2016, Parnas (using the Parnas Yahoo Account) sent and received various emails to and from another investor in Fraud Guarantee ("Victim-2"), including stating, "My brother please do the wire today as I explained the importance as far as everything else I told you we will work out when I get back and yes we will barter."

d. In or about October 2016, Correia, copying Parnas (at the Parnas Yahoo Account), exchanged various emails with another investor in Fraud Guarantee ("Victim-3") regarding wiring money to an account maintained by Parnas in order to satisfy his investment in Fraud Guarantee.

e. On or about April 13, 2017, Correia (using the Correia Yahoo Account) emailed Parnas (at the Parnas Yahoo Account) regarding certain communications with Victim-2.

f. In or about January and February 2018, Correia (using the Correia Yahoo Account), often copying Parnas (at the Parnas Yahoo Account), exchanged various emails with Victim-1, apparently concerning a potential different investment or transaction.

g. In or about March 2018, an investor in Fraud Guarantee ("Victim-5") exchanged emails with, among others, Correia (at the Correia Yahoo Account), concerning a $200,000 "loss" on his investment in Fraud Guarantee.

h. In or about July 2018, Parnas (at the Parnas Yahoo Account), along with Correia and others, received an invitation to participate in a phone call with a representative of [redacted] regarding Fraud Guarantee.

i. On or about September 18, 2018, Correia, blind copying Parnas (at the Parnas Yahoo Account), sent various Fraud Guarantee transactional documents to an investor in Fraud Guarantee ("Victim-4"). Several months later, on or about June 11, 2019, Correia forwarded this email to himself (at the Correia Yahoo Account).

j. On or about October 31, 2018, Correia emailed Parnas (at the Parnas Yahoo Account) concerning the negotiation of a Fraud Guarantee contract with [redacted]

k. In or about November 2018, Correia (using the Correia Yahoo Account) exchanged emails with Victim-1 regarding Victim-1's ownership stake in Fraud Guarantee.

l. In or about June 2019, Correia (using the Correia Yahoo Account), copying Parnas (at the Parnas Yahoo Account), exchanged emails with a third-party regarding certain unpaid expenses owed by Fraud Guarantee.

14. Therefore, there is probable cause to believe that the Parnas Yahoo Account and Correia Yahoo Account contain evidence of Correia's and Parnas's communications with each other regarding Fraud Guarantee, and with actual and potential victims of their fraudulent scheme.

15. Furthermore, based on my training and experience, email accounts like the Parnas Yahoo Account and Correia Yahoo Account, which have been used to communicate with others in furtherance of an unlawful fraudulent scheme, often contain records of that activity, including emails, chats, documents and multimedia (such as videos and photographs of documents or other evidence of criminality), payment records, contact information of co-conspirators and/or witnesses, notes about calls and meetings, calendar entries relating to calls and meetings, and internet search history relating to unlawful conduct. Additionally, email accounts like the Parnas Yahoo Account and Correia Yahoo Account often contain IP and location information, which can result in the creation of records of physical locations of meetings and calls. Individuals engaged in criminal activity often store such records in order to, among other things, keep track of co-conspirators' contact information, keep a record of requests for payments or of payments made, and follow-up on requests for payments, contributions, or other aspects of the schemes.

16. Accordingly, there is probable cause to believe that Subject Device-1, which contains content and information from the Parnas Yahoo Account and Correia Yahoo Account, will contain evidence of Parnas's and Correia's involvement in a fraudulent scheme involving Fraud Guarantee.

Subject Device-2
(Containing the Parnas iCloud Accounts)

17. Based on my review of electronic communications stored on the Parnas iCloud Accounts (obtained pursuant to the search warrants identified above), including text messages, iMessages, and WhatsApp messages, I have learned, in substance and in part, that Parnas engaged

in electronic communications with multiple individuals relevant to Fraud Guarantee. For example, the Parnas iCloud Accounts contain, among other things, evidence of communications between Parnas and (i) Correia, his principal co-conspirator in the Fraud Guarantee fraudulent scheme, (ii) Rudolph Giuliani, whom Parnas and Correia retained—through $500,000 paid by Victim-4—ostensibly to provide consulting services as to Fraud Guarantee, and (iii) various actual and potential investors in Fraud Guarantee, including Victim-1, Victim-2, Victim-3, Victim-4, Victim-5, and Intended Victim-1. These communications span from at least in or about early 2013 to in or about early 2019. Accordingly, there is probable cause to believe that these communications contain evidence and instrumentalities of the Subject Offenses, including discussions between Parnas and Correia concerning Fraud Guarantee and its business and operations (or lack thereof), discussions with Giuliani concerning his and his firm's work for Fraud Guarantee or other action taken in exchange for the $500,000 payment, and statements including representations or promises made to actual or potential victims of the fraudulent scheme.

18. Furthermore, based on my training and experience, iPhones like those linked to the Parnas iCloud Accounts, which have been used to communicate with others in furtherance of the Subject Offenses, often contain records of that activity, including call logs, voicemail messages, text messages, email correspondence, payment records, documents and multimedia (such as videos and photographs of documents or other evidence of criminality), contact information of co-conspirators and/or witnesses, notes about calls and meetings, internet search history relating to unlawful conduct, and logs of communication with co-conspirators and/or witnesses over messaging applications. Individuals engaged in criminal activity often store such records in order to, among other things, keep track of co-conspirator's contact information, keep a record of requests for payments or of payments made, and follow-up on requests for payments,

contributions, or other aspects of the schemes. Based on my training and experience, I also know that once records are backed up to an iCloud, they can exist there for months or even years after they were created, even if a user replaces an iPhone or removes files from an iPhone device. Indeed, I have learned from publicly-available information from Apple that, depending on a user's settings, even if a user removes files from an iPhone, that user would need to log into their iCloud account and manually delete those same files in order for them to be removed from the iCloud account. Accordingly, there is reason to believe that records will be found in the Parnas iCloud Accounts that date back years.

19. Accordingly, there is probable cause to believe that Subject Device-2, which contains content and information from the Parnas iCloud Accounts, will contain evidence of Parnas's and Correia's involvement in a fraudulent scheme involving Fraud Guarantee.

Subject Device-3 and Subject-Device-4
(Containing the Parnas iPhone 11 and Correia iPhone, Respectively)

20. Based on my review of electronic communications stored on the Parnas iCloud Accounts (obtained pursuant to the search warrants identified above), including text messages, iMessages, and WhatsApp messages, I have learned, in substance and in part, that Parnas used the Parnas Numbers associated with the Parnas iPhone 11 and Correia used the Correia Number associated with the Correia iPhone to engage in electronic communications with multiple individuals relevant to Fraud Guarantee. For example, the Parnas iCloud Accounts contain, among other things, evidence of communications between Parnas (using the Parnas Numbers) and Correia (using the Correia Number). The Parnas iCloud Accounts also contain evidence that the Parnas Numbers were used to send and receive group text messages amongst Parnas, Correia (using the Correia Number), and various actual and potential investors in Fraud Guarantee, including Victim-1, Victim-2, Victim-3, Victim-4, Victim-5, and Intended Victim-1. Accordingly, it appears that

much of the material stored on the Parnas iCloud Accounts was sent or received using the Parnas Numbers and therefore likely came from the Parnas iPhone 11. Thus, because (as set forth above) there is probable cause to believe that the Parnas iCloud Accounts contain evidence of Parnas's electronic communications with various individuals relevant to the Fraud Guarantee scheme, there is likewise probable cause to believe that evidence of such communications exists on Subject Device-3, which contains content and information from the Parnas iPhone 11.

21. Based on my review of documents produced by Victim-3, I have learned, in substance and in part, that Victim-3 engaged in extensive text message communications with Correia (who was using the Correia Number, which is associated with the Correia iPhone) concerning Fraud Guarantee, among other subjects, between at least in or about October 2016 and in or about October 2019. I have also learned from the CEO—including through my review of materials produced by him—that he was likewise in communication with Correia regarding Fraud Guarantee via text message between at least in or about early 2016 and late 2018. In addition, based on my review of documents produced by Victim-4, I have learned, in substance and in part, that Victim-4 exchanged text messages with Correia, concerning Victim-4's then-impending investment in Fraud Guarantee, between in or about September 16 and September 19, 2018.

22. Based on my review of technical information provided by Apple, I know that when an individual acquires a new iPhone, it is possible to transfer data from an old device to the new iPhone. Further, based on my training and experience, individuals regularly transfer such data so that they can have access to their contacts, messages, notes, calendar entries, and pictures, among other data. Accordingly, there is probable cause to believe that the Parnas iPhone 11 and Correia iPhone were used to send and receive the messages described above, or contain the backup or

transferred content from iPhones, and therefore are likely to contain evidence of Parnas's and Correia's electronic communications with these individuals.

23. In addition, based on my training and experience, individuals who engage in offenses such as the Subject Offenses often store records relating to their illegal activity and to persons involved with them in that activity on electronic devices such as the Parnas iPhone 11 and Correia iPhone. Such records can include, for example, logs of online chats or text messages or phone calls with co-conspirators; photographs, email correspondence and other communications (including via third-party messaging applications) with co-conspirators; contact information of co-conspirators, including telephone numbers, email addresses, and/or identifiers for instant messaging and social media accounts; financial data, including bank account numbers; and/or documents and drafts of documents used or contemplated for use in furtherance of the scheme.

24. Accordingly, there is probable cause to believe that Subject Device-3 and Subject Device-4, which contain content and information from the Parnas iPhone 11 and Correia iPhone, respectively, will contain evidence of Parnas's and Correia's involvement in a fraudulent scheme involving Fraud Guarantee.

* * *

25. Time limitation: To the extent materials are dated, this search warrant application is limited to all content created, sent, or received on or after September 1, 2013, which is shortly before Correia registered Fraud Guarantee in Delaware, to the present.

A. Evidence, Fruits and Instrumentalities

26. Based upon the foregoing, I respectfully submit there is probable cause to believe that the Subject Devices will contain evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachment A to the proposed warrant.

27. In particular, I believe the Subject Devices are likely to contain the following information:

a. Evidence relating to, including communications with, Rudolph Giuliani, [redacted] and any actual or potential investors, members, or partners of Fraud Guarantee;

b. Evidence relating to Fraud Guarantee's plans, finances, assets, and operations, or lack thereof, including any corporate books and records;

c. Evidence relating to Fraud Guarantee's actual or prospective business relationships, including but not limited to business relationships with any insurance carriers;

d. Evidence relating to Fraud Guarantee's members, officers, directors, investors, partners, employees, agents, consultants, affiliates, subsidiaries, and associates.

e. Evidence relating to the nature and extent of Rudolph Giuliani's and [redacted] work on behalf of Parnas, Correia, and/or Fraud Guarantee, or lack thereof, including any evidence of Giuliani's efforts to assist in the removal of Ambassador [redacted] and whether or not such efforts benefited Fraud Guarantee;

f. Evidence relating to any efforts by Parnas, Correia, their family members, or others associated with Fraud Guarantee in receiving, transferring, withdrawing, or otherwise using any monetary funds or instruments;

g. Evidence relating to the use of monetary funds or instruments paid to Fraud Guarantee, Parnas, or Correia to make political contributions;

h. Evidence of meetings between Parnas, Correia, Giuliani, and any actual or potential investors in Fraud Guarantee, including but not limited to travel records, and location and IP records;

i. Evidence of the existence of email accounts, iCloud accounts, or electronic devices used by Parnas, Correia or others associated with Fraud Guarantee to communicate with actual or potential investors, or co-conspirators;

j. Passwords or other information needed to access user's online accounts.

IV. Procedures for Searching ESI

A. Review of ESI

28. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, interpreters, and outside vendors or technical experts under government control) will review the ESI contained on the Subject Devices for information responsive to the warrant.

29. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by "opening" or reading the first few "pages" of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- "scanning" storage areas to discover and possibly recover recently deleted data or deliberately hidden files; and

- performing electronic keyword searches through all electronic storage areas to determine the existence and location of data potentially related to the subject matter of the investigation[1]; and

- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

30. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from seized devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

[1] Keyword searches alone are typically inadequate to detect all relevant data. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.

V. Conclusion and Ancillary Provisions

31. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

32. In light of the confidential nature of the continuing investigation, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.

[redacted]

Sworn to before me on
21st day of January, 2020

HON. J. PAUL OETKEN
UNITED STATES DISTRICT JUDGE

Attachment A

I. Devices to be Searched

The devices to be searched ("Subject Device-1," "Subject Device-2," "Subject Device-3," and "Subject Device-4," and collectively, the "Subject Devices") are described as four hard drive partitions containing the following content and information obtained pursuant to the following prior search warrants:

Account/Device	Previously searched pursuant to search warrant(s)	Referred to as
SUBJECT DEVICE-1		
[redacted]	19 Mag. 729 (Jan. 18, 2019) 19 Mag. 7593 (Aug. 14, 2019)	Parnas Yahoo Account
[redacted]	19 Mag. 7595 (Oct. 17, 2019)	Correia Yahoo Account
SUBJECT DEVICE-2		
Parnas iCloud account number [redacted]	19 Mag. 4784 (May 16, 2019) 19 Mag. 9829 (Oct. 21, 2019) 19 Mag. 9832 (Oct. 21, 2019)	Parnas iCloud Accounts
iCloud account number [redacted]		
SUBJECT DEVICE-3		
Black iPhone 11 with the serial number [redacted] seized from Lev Parnas incident to his arrest at Dulles International Airport on Oct. 9, 2019	19 Mag. 9832 (Oct. 21, 2019)	Parnas iPhone 11
SUBJECT DEVICE-4		
iPhone with the serial number [redacted] seized from a package sent by David Correia via DHL	19 Mag. 9830 (Oct. 21, 2019)	Correia iPhone

II. Review of ESI on the Subject Devices

Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, interpreters, and outside vendors or technical experts under government control) are authorized to review the ESI contained on the Subject Devices for evidence, fruits, and instrumentalities of one or more violations of 18 U.S.C. § 1343 (wire fraud) and § 1349 (attempting and/or conspiring to commit wire fraud) (together, the "Subject Offenses"), limited to content created, sent, or received between September 1, 2013 and the date of this warrant, as listed below:

a. Evidence relating to, including communications with, Rudolph Giuliani, [redacted] and any actual or potential investors, members, or partners of Fraud Guarantee;

b. Evidence relating to Fraud Guarantee's plans, finances, assets, and operations, or lack thereof, including any corporate books and records;

c. Evidence relating to Fraud Guarantee's actual or prospective business relationships, including but not limited to business relationships with any insurance carriers;

d. Evidence relating to Fraud Guarantee's members, officers, directors, investors, partners, employees, agents, consultants, affiliates, subsidiaries, and associates.

e. Evidence relating to the nature and extent of Rudolph Giuliani's and [redacted] work on behalf of Parnas, Correia, and/or Fraud Guarantee, or lack thereof, including any evidence of Giuliani's efforts to assist in the removal of Ambassador [redacted] and whether or not such efforts benefited Fraud Guarantee;

f. Evidence relating to any efforts by Parnas, Correia, their family members, or others associated with Fraud Guarantee in receiving, transferring, withdrawing, or otherwise using any monetary funds or instruments;

g. Evidence relating to the use of monetary funds or instruments paid to Fraud Guarantee, Parnas, or Correia to make political contributions;

h. Evidence of meetings between Parnas, Correia, Giuliani, and any actual or potential investors in Fraud Guarantee, including but not limited to travel records, and location and IP records;

i. Evidence of the existence of email accounts, iCloud accounts, or electronic devices used by Parnas, Correia or others associated with Fraud Guarantee to communicate with actual or potential investors, or co-conspirators;

j. Passwords or other information needed to access user's online accounts.

EXHIBIT A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

19 MAG 11651

In the Matter of a Warrant for All Content and Other Information Associated with the Email Accounts [redacted] and Maintained at Premises Controlled by Google, LLC, USAO Reference No. [redacted]

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

Agent Affidavit in Support of Application for a Search Warrant for Stored Electronic Communications

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

[redacted], being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). In the course of my experience and training in this position, I have participated in criminal investigations into federal offenses involving public corruption, including wire fraud and violations of the federal campaign finance laws. I also have training and experience executing search warrants, including those involving electronic evidence.

B. The Provider, the Subject Accounts and the Subject Offenses

2. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. § 2703 for all content and other information associated with the email accounts [redacted] ("Subject Account-1") and [redacted] ("Subject Account-2") (together, the "Subject Accounts"), maintained and controlled by Google, LLC (the

"Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrant.

3. As detailed below, there is probable cause to believe that the Subject Accounts contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud) and § 1349 (attempting and/or conspiring to commit wire fraud) (the "Subject Offenses"). This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers, as well as my training and experience concerning the use of email in criminal activity. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

C. Services and Records of the Provider

4. I have learned the following about the Provider:

a. The Provider offers email services to the public. In particular, the Provider permits subscribers to maintain email accounts under the domain name gmail.com or under any domain name under the subscriber's control. For example, if a subscriber controls the domain name "xyzbusiness.com," the Provider enables the subscriber to host any email address under this domain name (*e.g.*, "john@xyzbusiness.com"), on servers operated by the Provider. A subscriber using the Provider's services can access his or her email account from any computer connected to the Internet.

b. The Provider maintains the following records and information with respect to every subscriber account:

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on the Provider's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on the Provider's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the Provider's servers for a certain period of time.

ii. *Address book.* The Provider also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* The Provider collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. The Provider also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, the Provider maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Transactional information.* The Provider also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through the Provider's website).

v. *Google Drive Content.* The Provider provides users with a certain amount of free "cloud" storage, currently 15 gigabytes, through a service called "Google Drive" (users can

purchase a storage plan through Google to store additional content). Users can purchase enhanced storage capacity for an additional monthly fee. Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content "in the cloud" (that is, online). A user can access content stored on Google Drive by logging into his subscriber account through any computer or other electronic device connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

vi. *Google Docs.* The Provider provides users with the ability to write, edit, and collaborate on various documents with other users through a service called "Google Docs." Users can use Google Docs to create online documents that can be stored on or saved to the user's Google Drive.

vii. *Google Calendar.* The Provider provides users with an online calendar, in which they can add appointments, events, and reminders, which are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

viii. *Location History.* The Provider maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or "apps") or services provided by the Provider. For example, the Provider collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user's location. Provider-1 apps and services also allow for location reporting, which allows the Provider to periodically store and use a device's most recent location data in connection with a subscriber account.

ix. *Device Information.* The Provider collects and maintains information identifying devices (including both computers and mobile devices) used to access accounts,

including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI").

x. *Android Services.* The Provider also maintains information relating to Android, as it relates to an account. Android is a mobile operating system that is developed by the Provider, and is used on a variety of touchscreen mobile devices, such as smartphones and tablet computers. The Provider retains information related to the Android device associated with an account, including the IMEI (International Mobile Station Equipment Identifier), MEID (Mobile Equipment Identifier), device ID, and/or serial number of the device. Each of those identifiers uniquely identifies the device used. One device may be associated with multiple different Google and Android accounts, and one Google or Android account may be associated with multiple devices.

xi. *Cookie Data.* The Provider uses features to track the activity of users of their accounts, including whether or not the user of an account accesses other accounts at Google using the same computer, or accesses accounts maintained by other companies while logged into an account. One of the ways they do that is by using cookies, a string of characters stored on the user's computer or web browser that is recognized by Google when a computer visits its site or logs into an account.

xii. *Preserved and backup records.* The Provider also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon

receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). On or about November 11, 2019, the Government served the Provider with a preservation request for the Subject Accounts. The Provider may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

D. Jurisdiction and Authority to Issue Warrant

5. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

6. A search warrant under § 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

7. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

II. Probable Cause

A. Probable Cause Regarding the Subject Offenses

Overview

8. On or about October 9, 2019, a grand jury sitting in the Southern District of New York returned an indictment charging defendants Lev Parnas and Igor Fruman with conspiring to make